(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **G brauchsmusterschrift**

(10) **DE 200 14 381 U 1**

(51) Int. Cl.[7]:
H 04 L 9/32
H 04 M 11/00
G 07 C 9/00

(21) Aktenzeichen: 200 14 381.6
(22) Anmeldetag: 21. 8. 2000
(47) Eintragungstag: 30. 11. 2000
(43) Bekanntmachung im Patentblatt: 4. 1. 2001

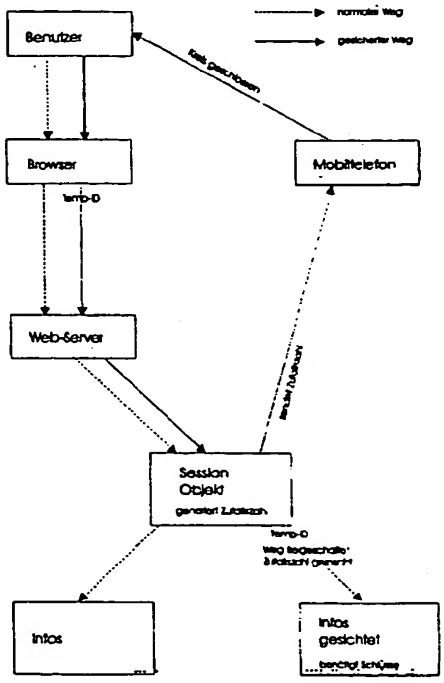
(73) Inhaber:
RENT A BRAIN GMBH, 73525 Schwäbisch Gmünd, DE

(74) Vertreter:
Ehrhart, M., Rechtsanw., 81927 München

(54) Vorrichtung zur Legitimationsprüfung

(57) Die Vorrichtung ist dadurch gekennzeichnet, dass die Prüfung einer Zugangsberechtigung dadurch erfolgt, dass ein ausschließlich temporärer Zugangscode durch einen Zufallsgenerator erzeugt und dann an ein personalisiertes Medium (Mobiltelefon, Pager) mittels Short Message Service (SMS) weitergeleitet wird.

Ablauf



DE 200 14 381 U 1

DE 200 14 381 U 1

17.10.00

BESCHREIBUNG

Vorrichtung zur Legitimationsprüfung

1 Einsatzgebiet

Es handelt sich um eine neuartige Legitimationsvorrichtung zum Beispiel für die Gewährung des Zugangs zu gesicherten Einrichtungen, welche einen erhöhten Sicherheitsstandard erfordern. Durch die Vorrichtung zur Prüfung der Zugangsberechtigung sollen ausschließlich hochsensible Bereiche innerhalb eines Systems geschützt werden.

2 Derzeitiger Stand der Technik:

Bisherige Legitimationsvorrichtungen basieren auf dem PIN / TAN – Verfahren oder auf sogenannten Smartcards. Diese Vorrichtungen konnten sich in der Vergangenheit durchsetzen, jedoch besitzen beide Legitimatiovorrichtungen technische Unzulänglichkeiten.

PIN ist eine persönliche Identifiktationsnummer, welche dem Benutzer eines Systems dauerhaft zugewiesen wird. Die Übermittlung der Nummer erfolgt in der Regel in schriftlich fixierter Form. Diese dauerhafte Form der Zugangsberechtigung birgt einige Risiken. Es besteht die Möglichkeit, dass durch die Versendung der PIN oder durch fahrlässiges Verhalten seitens des Benutzers die PIN – Nummer einer dritten Person zugänglich wird. Erfolgt nicht sogleich eine Sperrung dieser PIN ist ein Missbrauch nicht vermeidbar. Weiterhin erhöht sich mit dem dauerhaften Bestehen der PIN das Risiko ihrer Entschlüsselung.

TAN ist eine von vielen persönlichen Transaktionsnummern, welche jeweils nur für eine Transaktion benutzt werden kann. Die Gültigkeit einer TAN reicht von ihrer Erstellung bis zu ihrer Anwendung durch den Benutzer, das heißt der Zeitraum ihrer Gültigkeit hängt von ihrem Einsatz durch den Benutzer ab. TANs werden ebenso wie PINs in schriftlich fixierter Form auf dem Postweg versendet. Auch hier kann die TAN bei der Versendung oder durch fahrlässiges Verhalten seitens des Benutzers in die Hände Dritter gelangen. TANs sind zwar nicht dauerhaft gültig, jedoch sind sie auf Seiten des Dienstanbieters hinterlegt. Dadurch ist ein Missbrauch durch Mitarbeiter möglich.

Smartcard ist ein technisches Gerät, welches zeitgleich zum Server in festgelegten Z itintervallen di selb n Zugangscodes gen riert. Die Smartcard wiederum ist üb r inen PIN zugriffsgeschützt. All rdings erfordern Smartcards inen hohen

Verwaltungsaufwand, insbesondere bei der Erstausgabe von zum Teil mehrerer Tausend Smartcards oder bei der Sperrung von Zugriffsrechten. Benutzer von Smartcards müssen diese stets mit sich führen, um sich in das jeweilige System einloggen zu können. Ein Benutzer von mehreren Systemen muss somit zahlreiche Smartcards mit sich führen und sich damit für jede Smartcard die entsprechende PIN merken.

3 Funktion der Vorrichtung

Hier handelt es sich um eine Vorrichtung zur Prüfung der Zugangsberechtigung zu sensiblen Bereichen mittels Erzeugung eines ausschließlich temporären Zugangscodes und dessen Übermittlung an ein personalisiertes Medium.

Der Kern der Vorrichtung basiert auf Java, einer speziell für das Internet entwickelten objektorientierten Programmiersprache, auf Short Message Service (SMS), einem Versandprotokoll für Kurzmitteilungen über Mobiltelefone, sowie auf dem PIN-Schutz (Personal Identifikations Nummer) bei Mobiltelefonen.

Das Neuartige der Vorrichtung besteht darin, dass ein ausschließlich temporärer Schlüssel auf das Mobiltelefon des Benutzers übertragen wird. Der übermittelte Schlüssel berechtigt den Empfänger in sensiblen Bereichen einer Internetapplikation arbeiten zu können.

Beim Einloggen des Benutzers in den allgemein zugänglichen Bereich des Sicherheitsbereichs mittels Loginname und Passwort wird ein temporäres Javaobjekt[i] erzeugt, wobei der Konstruktor[ii] des Objekts den Zugangscode auf „NULL" und den Parameter zur Zugangskontrolle für diese Vorrichtung geschützte Bereiche auf „FALSE" setzt. Die vom Konstruktor gebildeten Datenelemente werden im Objekt gekapselt[iii] und sind damit nur über Methoden des Objekts ansprechbar. Diese Kapselung stellt einen sicheren Schutz vor unberechtigtem Datenzugriff dar, da die Datenelemente nicht direkt veränderbar bzw. auslesbar sind.

Das temporäre Javaobjekt existiert nur für die Dauer einer Session, der Arbeitsphase eines Benutzers vom Einloggen ins System bis zum Ausloggen, im RAM des Servers. Um einen sensiblen Bereich des Systems betreten zu können, muss der Benutzer eine Anfrage an das System stellen. In diesem Fall erzeugt das temporäre Javaobjekt selbständig einen temporären Zugangscode, welcher aus beispielsweise sieben, unabhängig voneinander generierten Zufallsziffern besteht. Dieser Zugangscode wird nun automatisch dem Benutzer per SMS zugesandt. Innerhalb von Sekunden nach seiner Anfrage kann der Benutzer den benötigten Zugangscode auf seinem SMS-fähigen Handy abrufen. Der übermittelte Zugangscode muss dann vom Benutzer in einer Dialogbox eingegeben werden, welche dem Javaobjekt übergeben wird. Stimmt der Zugangscode mit der Eingabe überein, wird vom Javaobjekt der Parameter zur Zugangskontrolle auf „TRUE" gesetzt. Dieser Parameter kann über ein allgemein zugängliche Methode des Objekts ausgelesen, jedoch nicht verändert werden. Der Benutzer bekommt dadurch für die restliche Zeit der Session Zugriff auf die mit der Vorrichtung geschützten

Ber iche. Der gesetzt Parameter ermöglicht es de. Benutzer innerhalb seiner S ssion beliebig zwisch n geschützten und allgemein zugänglichen Ber ichen ohn erneute Anforderung ein s Zugangscodes zu wechseln. Bei jedem versuchten Eintritt in einen durch diese Vorrichtung geschützt n Bereich wird vom System mittels einer Methode des Javaobjekts überprüft, ob der Parameter zur Zugangskontrolle den Zustand „TRUE" aufweist. Stimmt der Zugangscode mit der Eingabe nicht überein, wird der Zugangscode vom Javaobjekt gelöscht und damit eine erneute Anfrage des Benutzers notwendig.
Die Telefonnummer seines Mobiltelefons kann der Benutzer nur bei der Ersterstellung des persönlichen Benutzerprofils eingeben oder zu einem späteren Zeitpunkt innerhalb des geschützten Bereiches. Nur in dem mit dieser Vorrichtung geschützten Bereich kann eine Änderung der Telefonnummer vorgenommen werden. Sollte es zum Verlust des Handys seitens des Benutzers kommen, so kann der Benutzer nur noch per Antrag beim Dienstanbieter seine neue Handynummer für den mit der Vorrichtung geschützten Bereich einstellen lassen.

4 Vorteile gegenüber anderen Legitimationsvorrichtungen:

Der Vorteil von der beschriebenen Vorrichtung gegenüber einfachen PIN / TAN – Vorrichtungen liegt darin, dass die TAN – Nummer durch einen ausschließlich temporären Zugangscode ersetzt wird. Mit diesem Wegfall eines dauerhaft vorhandenen Codes entfällt die Gefahr des Datenmissbrauchs bei Verlust oder Entwenden des Codes durch einen Dritten. Da der temporär gültige Zugangscode von zu keinem Zeitpunkt auf einem permanenten Medium gespeichert wird und nur temporär im abgekapselten Bereich des Javaobjekts existiert, ist auch dem Dienstanbieter der derzeitige Zugangscode des Benutzers nicht bekannt. Er hat keine Möglichkeit des Zugriffs darauf, so dass ein Datenzugriff durch Mitarbeiter des Dienstanbieters ebenfalls weitestgehend ausgeschlossen werden kann.

Der Vorteil der Vorrichtung gegenüber Smartcards liegt darin, dass hier kein zusätzliches technisches Gerät vom Benutzer mitgeführt werden muss. Für den Zugang zu sensiblen Bereichen eines Sicherheitsbereichs benötigt der Benutzer lediglich sein Mobiltelefon. Daraus ergeben sich zweierlei Vorteile. Der Benutzer erhält durch sein PIN – geschütztes Mobiltelefon einen weiteren Schutz, muss sich jedoch keine weitere PIN – Nummer merken. Legitimationsvorrichtungen die mit Smartcards arbeiten bedeuten für den Dienstanbieter einen hohen Verwaltungsaufwand. Dieser entfällt bei der Arbeit mit dieser Vorrichtung.

Die Vorrichtung ist einfach bedienbar bei gleichzeitigem Schutz über mehrere Mechanismen. Um in sensible Bereiche des Systems zu gelangen, müsste ein Unbefugter Login und Passwort des Benutzers entschlüsseln, das Mobiltelefon des B nutzers entwend n und dessen PIN kennen.

5 Einsatzgebiete

Die beschriebene Vorrichtung kann überall dort eingesetzt werden, wo ein Zugangsberechtigung überprüft werden soll. Auf diesem Wege können alle die Systeme abgesichert werden, der n Zugang durch Eingabe eines alphanumerischen Codes ermöglicht wird. Anwendungsgebiete können somit sein: Zugang zu Sicherheitsbereichen (Türabsicherung), Geldautomaten, Kaufautomaten, Banktresore, Ausleihe wertvoller Güter, Aktionen in automatisierten Systemen.

---

[i] Siehe Abbildung „Javaobjekt"

[ii] Der Konstruktor bildet ein Objekt und nimmt die erste Initialisierung der Datenelemente vor.

[iii] Durch das Schlüsselwort „private" bei der Datenelementdeklaration werden die Datenelemente im Objekt gekapselt, das heißt von außerhalb des Objekts nicht ansprechbar.

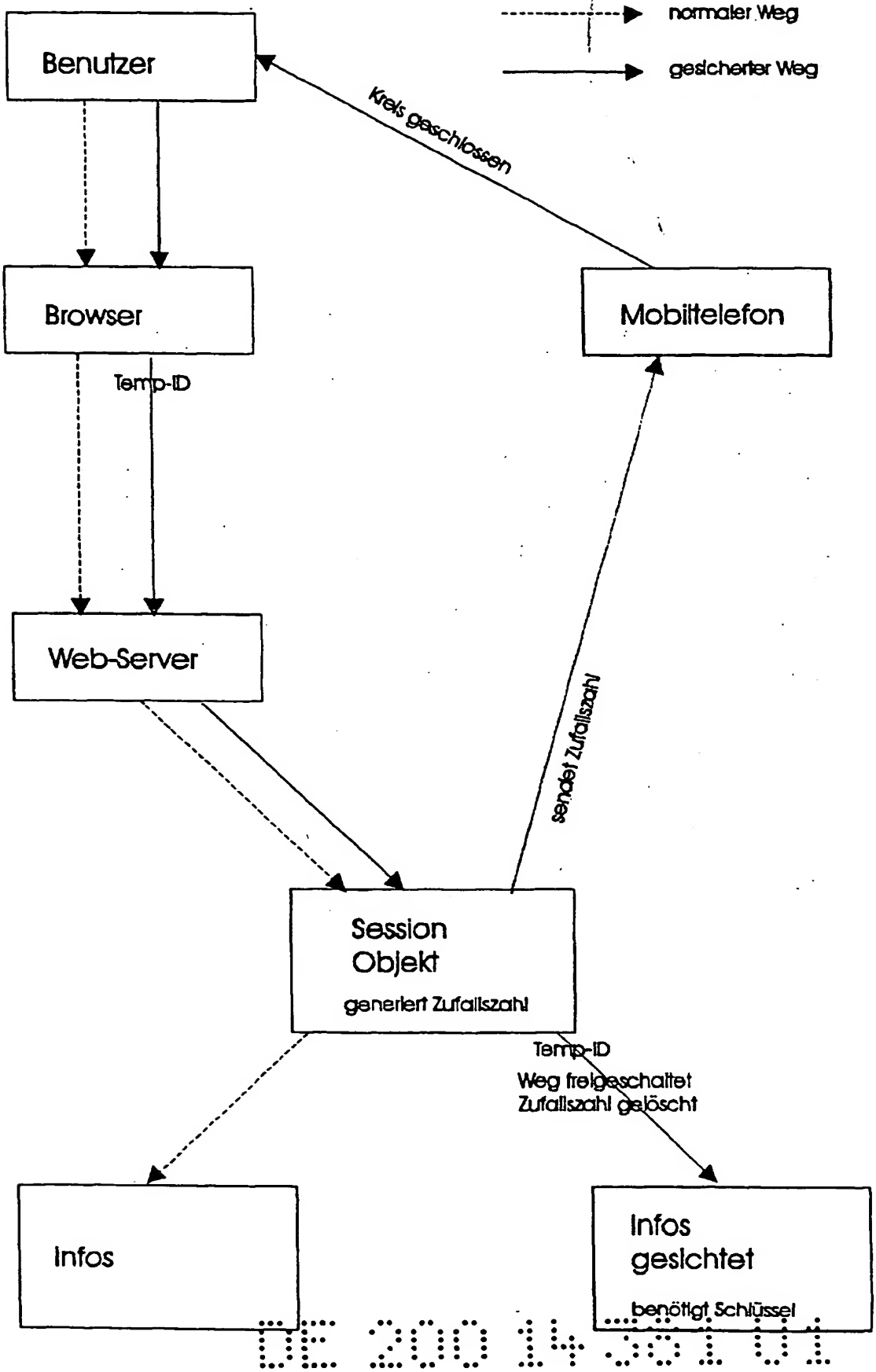
SCHUTZANSPRUCH

Vorrichtung zur Legitimationsprüfung

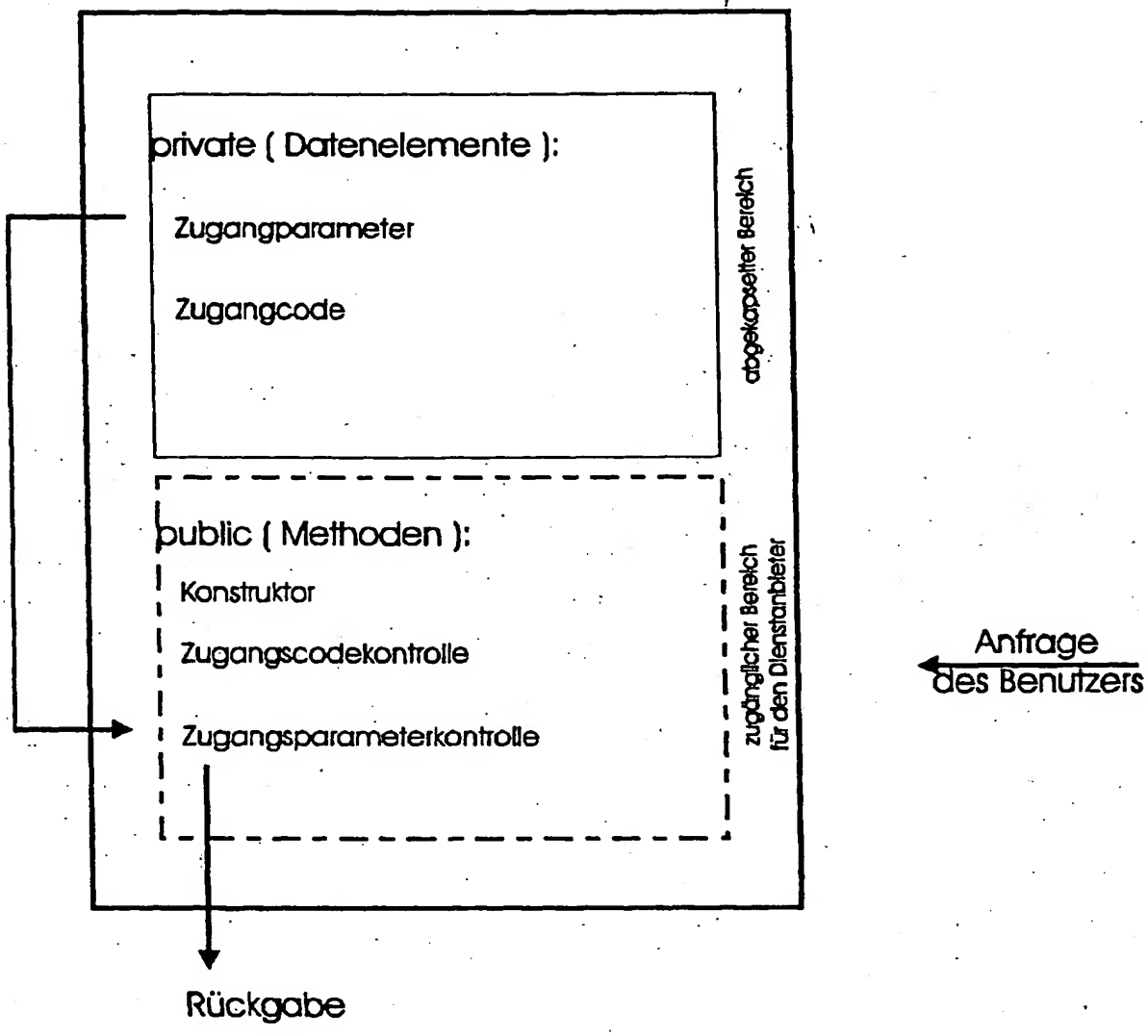
Die Vorrichtung ist dadurch gekennzeichnet, dass die Prüfung einer Zugangsberechtigung dadurch erfolgt, dass ein ausschließlich temporärer Zugangscode durch einen Zufallsgenerator erzeugt und dann an ein personalisiertes Medium (Mobiltelefon, Pager) mittels Short Message Service (SMS) weitergeleitet wird.

DE 200 14 381 U1

Ablauf



Java - Objekt



Zustände des Javaobjekts